



INFORMATION TECHNOLOGY & IMPLEMENTATION (SATELLITE)

21 November, 2023
Kyiv, Ukraine

Myroslav Dzekunov, master's degree student of the department of technologies management

Vadym Ziuziun, PhD, associate professor of the department of technologies management

Taras Shevchenko National University of Kyiv

METHODS OF COUNTERACTING THE OPERATION OF UNMANNED AERIAL VEHICLES THROUGH CYBERATTACKS ON CONTROL CHANNELS

Abstract. After the outbreak of the Russian-Ukrainian war, the world was forced to reconsider its approaches to defense and protection mechanisms. Immediately, different countries began to improve their existing weapons and develop new means to protect their territories and interests. This trend has not escaped unmanned aerial vehicles, which have a very significant impact on the course of the war in Ukraine. That is why there is a need to consider methods of countering enemy drones through cyberattacks.

Keywords: cyber security, drones (UAV), cyberattacks, channels, spoofing, network protocol, GPS signal.

Introduction. Since it is not always possible to purchase well-protected military drones in war, the military sometimes uses ordinary civilian drones. Often, the manufacturers of ordinary drones sold in stores do not protect them with encryption, and unencrypted data is an easy target for attackers.

Perhaps the most important components of UAVs exposed to cyberattacks are software systems, data transmission technologies and control channels. Among the software systems used by UAVs; autonomous driving software, image recording and processing software, map software, control center software and security software. Different signals, protocols and technologies are used between communication centers [1].

Cyberattacks on UAV control channels. There are several ways to hack a drone. An attacker can, for example, replace the GPS signal. Having received other coordinates, the drone will cancel the original route and fly to wherever the new owner orders. A drone can be hacked even from a kilometer away. If the radio signal is not encrypted, it can be easily decoded using a special program - a traffic analyzer (sniffer). This does not require any special technical skills or equipment. By intercepting the signal from the operator, the hacker gains full control over the drone and its systems. The signal can also be jammed, making the drone forget the request of the real owner. Below is a list of possible cyberattacks on drone control channels:

- **Signal Interception:** This attack involves intercepting radio signals transmitted between the UAV and the ground control station. Attackers can use specialized equipment to collect signals and determine the movements and actions of the vehicle.

- **Signal Spoofing:** In this attack, attackers create fake radio signals that mimic legitimate operator commands. This can cause the UAV to lose communication with the ground station [2].
- **DoS:** These attacks aim to overload the communication channels or infrastructure associated with the UAV with a large number of requests or traffic. This can lead to a loss of access to the vehicle.
- **GPS Spoofing:** With this attack, attackers can try to change the GPS coordinates that the UAV receives. This can lead to incorrect navigation of the vehicle and its deviation from the planned route.
- **Data Injection:** Attackers may try to inject fake data into the communication flow between the UAV and the ground control station.
- **Authentication Bypass:** Attackers may attempt to bypass or hack authentication and authentication systems to gain unauthorized access to the UAV's control system and issue their own commands.
- **Physical Attacks:** Physical access to UAV-related equipment or infrastructure can lead to technical interference, loss of the vehicle, or even hijacking.
- **Security Infrastructure Attacks:** Aimed at weakening or bypassing security and defense systems, including firewalls, intrusion detectors, and identification systems.
- **Network Protocol Attacks:** Attacks that target vulnerabilities in network protocols used for communication, including attacks on TCP/IP, UDP, and other network protocols.
- **Software Vulnerabilities:** Attackers can exploit vulnerabilities in the UAV control system software to launch attacks and gain control of the vehicle.

References:

1. The fight against attack UAVs of the Iranian and Russian military production «Shahed-136» («Geranium-2») and «Lancet-2». Methodical recommendations for illegal pedophiles (based on the evidence of the Russian-Ukrainian war of 2022-2023), 2023.
2. Cyber Attacks on Unmanned Aerial Vehicles and Cyber Security Measures // The Eurasia Proceedings of Science, Technology. – 2022. – URL: <http://www.epstem.net/tr/download/article-file/2860741>. Access date: 25.10.2023.
3. Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles // Xu, W., Yan, Chen, J., Jia, W., Ji, X., Liu, J. – 2018. – URL: https://www.researchgate.net/publication/327324550_Analyzing_and_Enhancing_the_Security_of_Ultrasonic_Sensors_for_Autonomous_Vehicles. Access date: 23.10.2023.
4. Security, Privacy, and Safety Aspects of Civilian Drones: A Survey // ACM Transactions on Cyber-Physical Systems. – 2016. – URL: <https://dl.acm.org/doi/10.1145/3001836>. Access date: 23.10.2023.

TARAS SHEVCHENKO NATIONAL UNIVERSITY OF KYIV
(FACULTY OF INFORMATION TECHNOLOGY,
FACULTY OF COMPUTER SCIENCE AND CYBERNETICS)
NATIONAL TECHNICAL UNIVERSITY OF UKRAINE
“IGOR SIKORSKY KYIV POLYTECHNIC INSTITUTE”
VIKTOR GLUSHKOV INSTITUTE OF CYBERNETICS OF THE NAS OF UKRAINE
INSTITUTE FOR INFORMATION RECORDING OF THE NAS OF UKRAINE
INSTITUTE OF SOFTWARE SYSTEMS OF THE NAS OF UKRAINE
THE COUNCIL OF YOUNG SCIENTISTS OF THE FACULTY OF COMPUTER SCIENCE AND
CYBERNETICS AND THE FACULTY OF INFORMATION TECHNOLOGY OF
TARAS SHEVCHENKO NATIONAL UNIVERSITY OF KYIV
PUBLIC ASSOCIATION «COGNITIVE RESEARCH»

X INTERNATIONAL CONFERENCE

Information Technology and Implementation (Satellite)

21 November, 2023

Conference Proceedings

Kyiv

2023

UDC 004.9
I-74

Volume editor: Vitaliy Snytyuk, Dr.Sc., Prof.

Program Committee: Aldrich Chris, Andreas Pester, Frederic Mallet, Hiroshi Tanaka, Iurii Krak, Yulia Khlevna, Karsten Henke, Oleg Chertov, Oleksandr Kuchanskyi, Oleksandr Marchenko, Sándor Bozóki, Vitaliy Tsyganok, Vladimir Vovk

Organizing Committee: Anatoly Anisimov, Vitaliy Snytyuk, Oleksii Bychkov, Oleh Ilarionov, Yurii Kravchenko, Iurii Krak, Oleksandr Kuchanskyi, Oleksandr Marchenko, Viktor Morozov, Taras Panchenko, Iryna Rozora, Valentyna Pleskach, Yurii Samokhvalov, Oleksii Tkachenko, Serhii Toliupa.

Conference Secretary: Hryhorii Hnatiienko.

I-74 Information Technology and Implementation (Satellite): Conference Proceedings, November 21, 2023, Kyiv, Ukraine / Ministry of Education and Science of Ukraine, Taras Shevchenko National University of Kyiv and [etc]; Vitaliy Snytyuk (Editor). – Kyiv: Publishing House «Caravela», 2023. 343 p.

ISBN 978-960-801-907-4

This book includes abstracts of the 10th International Conference "Information Technology and Implementation (Satellite) – 2023". Philosophical, theoretical and applied aspects which describe the results, problems and prospects of the creation and use of intelligent computing methods and creating of information systems and technology on their basis are reviewing.

Main tracks of the conference are: Artificial Intelligence Technologies, Cyberspace Protection Technologies, Data Analytics, Digital Project Management Technologies, E-commerce, E-government and E-learning Technologies, Mathematical Foundations of Information Technology, Network and Internet Technologies, Smart Technologies.

До цієї збірки увійшли тези 10-ї Міжнародної конференції «Інформаційні технології та впровадження (сателітної) – 2023». Розглядаються філософські, теоретичні та прикладні аспекти, які описують результати, проблеми та перспективи створення і використання інтелектуальних обчислювальних методів та створення на їх основі інформаційних систем і технологій.

Основні напрямки конференції: Технології штучного інтелекту, Технології захисту кіберпростору, Аналітика даних, Технології цифрового управління проєктами, Електронна комерція, Електронне урядування та Технології електронного навчання, Математичні основи інформаційних технологій, Мережеві та Інтернет-технології, Розумні технології.

UDC 004.9

ISBN 978-960-801-907-4

© Authors of abstracts, 2023

<i>Mykhailo Otmorskyy, Andrii Roskladka, Vitalii Lazorenko. Using information technologies in the study and assessment of human behavior</i>	191
<i>Vladyslav Pelishenko, Yuliya Khlevna. Utilizing deep learning for detection of disinformation in social networks</i>	194
<i>Nikita Podolskyi, Andrii Khlevnyi. Development of Data Science technology in customer segmentation using support vector machine classification method</i>	197
<i>Dmytro Prokhorchuk, Andrii Khlevnyi. Heart rate variability analysis software</i>	199
<i>Mariia Pryidun, Yulia Khlevna. Data Science technologies for emotional analysis</i>	201
<i>Yevhenii Rudkivskyi, Andrii Khlevnyi. Software for recognizing ships on digital images</i>	203
<i>DIGITAL PROJECT MANAGEMENT TECHNOLOGIES</i>	205
<i>Dmytro Bredikhin, Vadym Ziuziun. Substantiation of the approach to the creation of an information system for calculating fuel consumption and carbon dioxide emissions by motor vehicles</i>	206
<i>Oleksandr Brova, Iryna Yurchuk. Flexible recognition of geographical objects in photographs of the Earth's surface</i>	210
<i>Myroslav Dzekunov, Vadym Ziuziun. Methods of counteracting the operation of unmanned aerial vehicles through cyberattacks on control channels</i>	213
<i>Andrii Ivko. Business and data understanding in realize phases of syncretic methodology</i>	215
<i>Andrii Korutchak, Vadym Ziuziun. Project management in the development of an e-commerce platform using artificial intelligence methods</i>	219
<i>Viktor Kulkovets, Liubov Kubiavka. Development of innovative mobile applications for improving education: from technology to knowledge</i>	221
<i>Bohdan Oryshchak, Andrii Khlevnyi. A WEB-based platform to improve the coordination of volunteerism</i>	223
<i>Riaz Dava Khan Sanaulla, Bohdan Yeremenko. Cybersecurity management in information technology projects- implementation</i>	227
<i>Yehor Striletskyi, Viktor Morozov. Study of problems of the furniture manufacturing ERP-system development project</i>	229
<i>Kateryna Valko, Liubov Kubiavka. Development of a concept for creating a platform for ukrainian manufacturers using project management practices</i>	233
<i>Artem Yurechko, Denys Liashenko, Ilya Taiurskyi, Oleksandr Timinskyi. Advantages of working with data in headless CMS over traditional CMS</i>	235